



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,434	08/30/2000	Douglas B. Moran	RECOP014	2556

21912 7590 03/18/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER

HENEGHAN, MATTHEW E

ART UNIT PAPER NUMBER

2134

DATE MAILED: 03/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/651,434		MORAN, DOUGLAS B.	
	Examiner		Art Unit	
	Matthew Heneghan		2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2000 and 14 November 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 August 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-17 have been examined.

Priority

The following is a quotation of the appropriate part of 35 U.S.C. 120:

An application for patent for an invention disclosed in the manner provided by the first paragraph of section 112 of this title in an application previously filed in the United States, or as provided by section 363 of this title, which is filed by an inventor or inventors named in the previously filed application shall have the same effect, as to such invention, as though filed on the date of the prior application, if filed before the patenting or abandonment of or termination of proceedings on the first application or on an application similarly entitled to the benefit of the filing date of the first application and if it contains or is amended to contain a specific reference to the earlier filed application.

2. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows: the application to which the instant application has been filed as a continuation, U.S. Patent Application No. 09/615,967, filed 14 July 2000, has no inventors in common with the instant application.
3. The instant application claims priority to Provisional U.S. Patent Application No. 60/151,531, filed 30 August 1999.

Information Disclosure Statement

4. The following Information Disclosure Statement in the instant application has been fully considered:

Paper No. 5, filed 16 April 2001.

5. Three additional documents have been found in the file wrapper that were not listed on the Form PTO-1449:

Lunt, et al., "Automated Audit Trail Analysis and Intrusion Detection: A Survey," October, 1988.

Farmer et al., "The COPS Security Checker System," 1990.

Porras et al., "EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances," date unknown.

Each has been fully considered.

Drawings

6. The drawings are objected to under 37 CFR 1.74 and 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, reference numbers for the claimed features, as depicted in Figure 9, must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

7. The drawings are objected to as failing to comply with 37 CFR 1.84(l) because the lines in Figure 2 are not uniformly thick and well-defined. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-6, 11, and 13 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,530,757 to Krawczyk.

As per claim 1, Krawczyk computes fingerprints (signatures) for each file and archives them. Fingerprints can be stored in multiple locations. Signatures are later retrieved and correlated (see abstract and column 5, lines 4-36).

As per claims 2-4, 11, and 13, one set of fingerprints may be stored on one or more remote servers, in what would constitute a package management database; another set may be stored internally (see column 2, line 58 to column 3, line 16).

As per claim 5 and 6, one of the fingerprints is stored in the archives using a one-way hash function. The other set must therefore be stored using a different algorithm, in order to allow for later decryption (see column 4, line 55 to column 5, line 2).

9. Claims 7, 8, 12, and 14 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,572,590 to Chess.

The method for discriminating malicious changes disclosed by Chess includes derived signatures that are tested against a set of rules (a database of exceptions) after differences have been determined (see abstract and column 5, lines 8-23).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,572,590 to Chess.

Regarding claim 9, Chess does not specifically disclose a rule that discriminates by file types, as the data has already been sorted by file type before the application of

the rules, suggesting that this is to divide objects according to their internal structure (see column 3, lines 37-43).

Chess also states that rules establish criteria for determining whether or not an analysis of the set of differences indicates change (see column 5, lines 12-14 and 38-44).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Chess by creating a rule that discriminates by file type, instead of pre-sorting the files, in order to divide objects according to their internal structure.

As per claim 10, the rules may determine whether a change is malicious, probably malicious, or neither (see column 5, lines 12-37).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,349,655 to Mann discloses the comparing of file fingerprints to assist in restoration.

U.S. Patent No. 5,826,013 to Nachenberg discloses a system for matching virus-infected files against various rules.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:


(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

MEH

March 4, 2004


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100